Traps: Hochentwickelter Schutz für Endpoints

TRAPS:

- **Verhindert Exploits für alle Schwachstellen**
- **Verhindert alle malwarebasierten Angriffe**
- **Liefert sofort Forensikdaten für abgewehrte Angriffe**
- **Skalierbar, leicht und benutzer-freundlich**
- **Integration mit Netzwerk- und Cloud Security**

Palo Alto Networks® Traps bietet hochentwickelten Schutz für Endpoints zur Verhinderung ausgefeilter Schwachstellen-Exploits und malwarebasierten Angriffen. Traps nutzt hierzu einen hoch skalierbaren, leichten Agenten mit einem neuen Ansatz zur Angriffsabwehr, der keinerlei Vorab-Kenntnisse übe die Bedrohung selbst erfordert. Das macht Traps für Organisationen zu einem leistungsfähigen Werkzeug, um Endpoints vor allen gezielten Angriffen zu schützen.

Palo Alto Networks Traps nutzt einen einzigartigen Ansatz zum Thema Endpoint-Sicherheit, der dazu entwickelt wurde, Endpoints vollständig zu schützen, einschließlich Abwehr sowohl bekannter Angriffe als auch hochentwickelter und gezielter Angriffe, vor denen herkömmliche Lösungen keinen Schutz bieten können.

Anstatt zu versuchen, die Millionen Einzelangriffe selbst zu identifizieren, oder schädliches Verhalten aufzuspüren, das nicht erkennbar ist, konzentriert sich Traps auf die Kerntechniken, die jeder Angreifer zusammenführen muss, um einen Angriff auszuführen. Durch den Aufbau einer Reihe von „Fallen“ zur Abwehr dieser Techniken ist Traps in der Lage, den Angriff sofort abzuwehren, bevor irgendeine schädliche Aktivität erfolgreich ausgeführt werden kann.

Durch diesen einzigartigen Ansatz ist Traps applikationsunabhängig und schützt alle Applikationen, auch solche, die von Dritten entwickelt wurden.

Verhinderung von Exploits

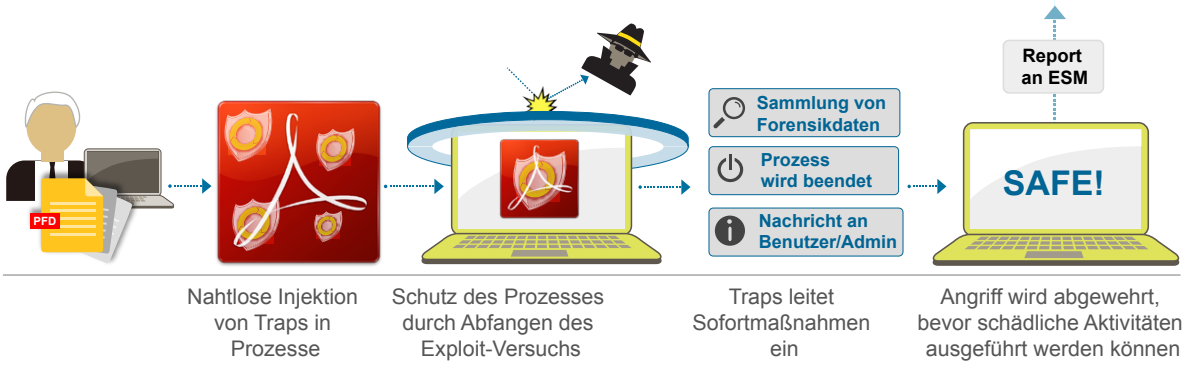
Der eigentliche Vorgang, bei dem eine Schwachstelle auf einem Endpoint ausgenutzt wird, erfordert die Ausführung mehrerer hochentwickelter Techniken hintereinander. So versucht ein Angreifer bei einer typischen Attacke beispielsweise zunächst, die Speicherzuweisung oder Handler zu beschädigen oder zu umgehen, um sie Kontrolle über ein System zu erlangen. Mit Hilfe von Techniken, die den Speicher beschädigen, wie z.B. Pufferüberlauf oder Heap Corruption, kann der Hacker Schwächen oder Schachstellen in der Zielsoftware ausnutzen, um seinen speziellen Code auszuführen. Ist der Angreifer erst einmal in der Lage, individuellen Code auszuführen, kann er Malware herunterladen oder das komplette Systemen nach seinem Willen steuern.

Unabhängig vom Angriff oder dessen Komplexität gilt: für einen erfolgreichen Angriff muss der Angreifer eine Reihe von Exploit-Techniken hintereinander ausführen. Manche Angriffe erfordern dabei mehr Schritte, andere weniger, aber in jedem Fall müssen mindestens zwei oder drei Techniken angewandt werden, um den entsprechenden Endpoint zu kapern.

So funktioniert die Abwehr von Exploits

Traps nutzt einer Reihe von Abwehrmodulen für Exploits, deren Zweck die Abwehr und das Blockieren der unterschiedlichen Exploit-Techniken ist, die den Hackern zur Verfügung stehen. Diese Module dienen als „Fallen“, die in

paloalto networks



Funktionsweise: Abwehr von Exploits.

den Benutzerprozess injiziert werden und die Exploit-Technik des Angreifers abblocken, sobald ein Angriffsversuch gestartet wird. Sobald eine Applikation geöffnet wird, injiziert Traps nahtlos die Abwehrmodule als transparente, statische "Fallen" in den Prozess, der dann vor allen Exploits geschützt ist. Wird ein Exploitversuch mit Hilfe der wenigen noch verbleibenden Techniken gestartet, blockiert Traps diese Technik sofort, beendet den Prozess uns benachrichtigt sowohl den Benutzer als auch den Administrator über den abgewehrten Angriff. Zusätzlich sammelt Traps detaillierte Forensikdaten und übermittelt diese Information an den Endpoint Security Manager (ESM). Aufgrund des kettenartigen Aufbaus eines Exploits muss man lediglich eine der Techniken in der Kette abwehren, um den gesamten Angriff zu verhindern.

Erfolgt kein Angriffsversuch, läuft für den Benutzer und den Prozess alles wie gewohnt. Da Traps nur minimale Ressourcen benötigt, wird das Benutzererlebnis durch die Abwehrmaßnahmen hinter den Kulissen in keiner Weise beeinträchtigt.

Durch die Konzentration auf die Kerntechniken anstelle des eigentlichen Angriffs ist Traps in der Lage, Angriffe ohne vorherige Kenntnis der Schwachstelle abwehren, unabhängig von vorhandenen Patches, und ohne Signaturen oder Softwareupdates. Wichtig ist hierbei, dass Traps keine Scans oder Überwachung von schädlichen Aktivitäten ausführt, was enorme Vorteile bei der Skalierbarkeit mit sich bringt, da äußerst wenig CPU und Speicher benötigt werden.

Die Exploit-Abwehr von Traps wurde entwickelt, um Angriffe auf Programmschwachstellen zu verhindern, die auf Speicherkorruption oder Logikfehlern basieren. Hier einige Beispiele für Angriffe, die Traps abwehren kann:

- Speicherkorruption
- Ausführung von Java-Code in Browsern, unter bestimmten Bedingungen
- Erzeugung von Child-Prozessen durch ausführbare Dateien, unter bestimmten Bedingungen
- Kapern von Dynamic Link Libraries (DLL) (Ersetzen einer rechtmäßigen DLL durch eine schädliche mit dem gleichen Namen)
- Kapern der Programmsteuerung
- Einfügen von Schadcode als Exception Handler

Abwehr von Malware

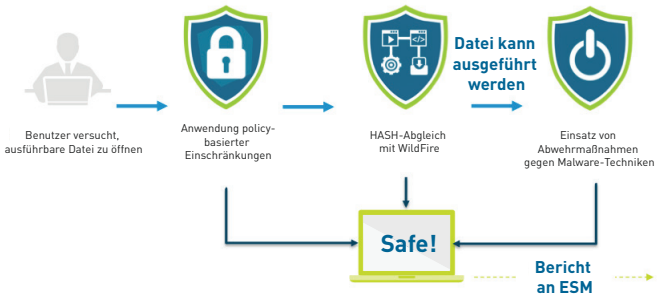
Schädliche ausführbare Dateien, auch als Malware bekannt, werden oftmals als gutartige Dateien getarnt oder sind in diesen eingebettet. Diese Dateien können den Computer beschädigen, indem sie versuchen, die Kontrolle zu übernehmen, sensible Informationen zu sammeln oder den normalen Betrieb des Systems stören.

Während gewiefte Angreifer verstärkt Schwachstellen in Software ausnutzen, entwickeln sich die Angriffe auch über unbekannte oder manipulierte Malware weiter (ausführbare Dateien). Da diese Angriffsarten im Allgemeinen keine bekannten Signaturen, bekannte Zeichenfolgen oder bekanntes Verhalten aufweisen, sind herkömmliche Ansätze zur Endpoint-Sicherheit nicht in der Lage, diese zu verhindern.

Um die Ausführung von Malware auf dem Endpoint effektiv zu verhindern, nutzt Traps die drei folgenden Komponenten für den Malwareschutz:

1. **Policy-basierte Beschränkungen: damit sind Organisationen in der Lage, Richtlinien zu erstellen, welche spezifische Ausführungs-Szenarien beschränken, anstatt bestimmte Dateien auf eine Blacklist oder Whitelist zu setzen. Die Angriffsfläche kann bedeutend verringert werden, indem man einfach die** Installationsquelle der Datei kontrolliert. Versucht ein Benutzer, die ausführbare Datei zu öffnen, bewertet Traps die entsprechenden Regeln zur Einschränkung. Beispiele für gängige policy-basierte Einschränkungen:
   - Öffnen von ausführbaren Dateien aus bestimmten Ordnern
   - Öffnen von ausführbaren Dateien aus externen Medien
   - Prozesse, die Child-Prozesse erzeugen
   - Java-Prozesse aus Browsern
   - Ausführen unsignierter Prozesse
   - Thread Injection

2. **Wildfire™ Inspection:** Für die Ausführung von Dateien, die nicht auf die geltenden Einschränkungen beschränkt sind, fragt der Traps Endpoint Security Manager mit einem Hash die WildFire Cloud ab, um festzustellen, ob die Datei schädlich, gutartig oder in der globalen Threat Community unbekannt ist. Falls Wildfire die Datei als bekannte Malware bestätigt, verhindert Traps die Ausführung der Datei und benachrichtigt den ESM.
3. Abwehr von **Malware-Techniken:** Ähnlich wie bei den Exploit-Techniken nutzen Angreifer gängige und identifizierbare Techniken zum Absetzen ihrer Malware. Falls die Ausführung einer Datei nicht über die Richtlinien beschränkt ist, oder nicht per Hash in der Wildfire Threat Cloud als bekannte Malware bestätigt wurde, implementiert Traps technikbasierte Gegenmaßnahmen zur Einschränkung bzw. Blockierung - Child-Prozesse, Java-Prozesse, die in Webbrowsern gestartet werden, Erstellung von Remote Threads oder Prozessen und die Ausführung unsignierter Prozesse - um den Angriff von vornherein komplett zu verhindern.



Funktionsweise: Abwehr von Malware

Forensik

Immer, wenn Traps einen Angriff verhindert, werden in Echtzeit Forensikdaten zu dem Ereignis gesammelt: Datei, Vorgänge, Speicherzustand beim Auftreten des Ereignisses etc. Diese Informationen werden dann als Protokoll an den Endpoint Security Manager (ESM) übermittelt. Trotz der Tatsache, dass der Angriff verhindert wurde, lässt sich hier immer noch eine Menge Information sammeln. Durch die Aufzeichnung aller forensischen Daten zum jeweiligen Angriff können Organisationen ihre Abwehrmaßnahmen proaktiv auf alle Endpoints ausweiten, die eventuell nicht geschützt sind.

Traps Architektur

Traps verfügt über eine 3-stufige Managementstruktur. Diese umfasst den Endpoint Security Manager, des Endpoint Connection Server und Endpoint Agents. Dieses Modell erlaubt eine massive horizontale Skalierbarkeit bei gleichzeitiger zentraler Konfiguration und Datenbank für Policies, Forensik etc.

Endpoint Security Manager

Der Endpoint Security Manager liefert ein administratives Dashboard für das Management von Sicherheitsvorfällen, Endpoint-Zustand und Policy-Regeln. Der ESM übernimmt auch die Kommunikation mit WildFire , wenn Hashes zur Prüfung übermittelt werden. Das ESM All-in-One Management Center umfasst:

- Konfigurationsmanagement
- Logging und DB-Abfrage
- Admin-Dashboard und Security-Übersicht
- Aufzeichnung von Forensikdaten
- Integrationskonfiguration

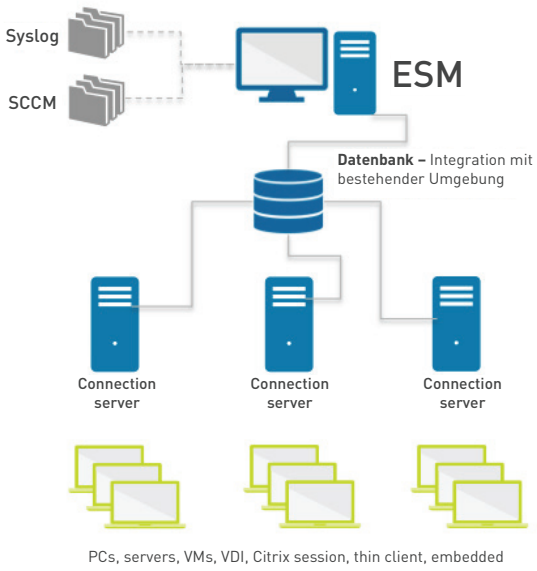
Der Endpoint Security Manager beinhaltet eine zentrale Datenbank zur Speicherung von administrativen Informationen, Policy-Regeln, Endpoint-Historie und weiteren Informationen zu sicherheitsrelevanten Ereignissen. Die Datenbank wird über die MS-SQL-Plattform gemanagt.

Der Endpoint Security Manager kann Protokolle auf externe Protokoll-Plattformen schreiben, z.B. Security Information and Event Management (SIEM), Service Organization Controls (SOCs), oder Syslog, und kann die Protokolle zusätzlich intern abspeichern. Die Angabe einer externen Logging-Plattform ermöglicht einen aggregierten Überblick der Protokolle von allen Endpoint-Servern.

Endpoint Server

Der Endpoint Server distributiert regelmäßig die Sicherheitsrichtlinie an alle Agents und managt die gesamte Information bezüglich sicherheitsrelevanter Ereignisse.

- **Traps Status** – Benachrichtigungen und Statusseiten im Endpoint Security Manager zeigen den Status für jeden Endpoint.
- **Benachrichtigungen** – Der Traps Agent schickt Benachrichtigungen zu Änderungen am Agent, z.B. Start oder Stopp von Services, an den Endpoint Server.
- **Abwehr-Reports** – Traps meldet alle Informationen zu einem Ereignis in Echtzeit an den Endpoint-Server.a



Abdeckung & unterstützte Plattformen

Traps schützt ungepatchte Systeme, erfordert keine Hardware und wird auf allen Plattformen unterstützt, auf denen Microsoft Windows läuft: Desktops, Server, Industriesteuerungen, Terminals, VDI, VMs, eingebettete Systeme etc.

Traps unterstützt aktuell die folgenden Windows-basierten Betriebssysteme:

WORKSTATIONS

- Windows XP SP3
- Windows 7
- Windows 8.1
- Windows Vista SP1

SERVER

- Windows Server 2003
- Windows Server 2008 (+R2)
- Windows Server 2012 (+R2)

Spezifikationen

Dank des einzigartigen Ansatzes funktioniert Traps eher statisch und scannt nicht auf schädliche Aktivitäten. Der Ressourcenverbrauch liegt äußerst niedrig:

TRAPS AGENT:

- CPU – Durchschnittliche Nutzung von 0,1%
- Speicherbedarf – 25 MB
- Festplattenbedarf – 15 MB

paloalto networks
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com